

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 SUBJECT FILES stored on a thumb drive in the
 custody of the Federal Bureau of Investigation in
 Bellingham, WA (more fully described in Att. A)

Case No. MJ25-050

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

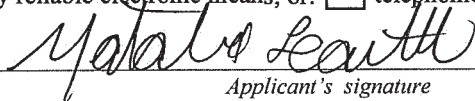
<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252(a)(2)	Receipt or distribution of child pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of/access with intent to view child pornography

The application is based on these facts:

- ☒ See Affidavit of FBI Special Agent Natalie Leavitt, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Natalie Leavitt, Special Agent, FBI
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/30/2025


Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)

) ss

COUNTY OF WHATCOM)

I, Natalie Leavitt, being duly sworn on oath, depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2022. I am currently assigned to the Bellingham Resident Agency of the Seattle Division and the FBI's Northwestern Washington Safe Trails Task Force ("NWSTTF"). I have attended several training courses including but not limited to Human Trafficking Investigations in September of 2024 and Human Trafficking in Indian Country in April of 2023. My primary responsibilities as a Special Agent include investigations involving violent crimes and other federal crimes on the Indian reservations in Northwest Washington. My duties as a special agent also include the investigation of those engaged in the sexual exploitation of children including the production, attempted production, distribution, and possession of child pornography. I have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256(8), in various forms of media, including media stored on digital media storage devices such as computers, iPhones, etc. I have participated in the execution of numerous search warrants which involved child exploitation and/or child pornography offenses.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the SUBJECT FILES associated with CyberTipline Report 197075910, more fully described in Attachment A, for the things specified in Attachment B to this Affidavit, for the reasons set forth below.

3. The warrant would authorize a search of the SUBJECT FILES for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of/Access with Intent to View Child Pornography) (the TARGET OFFENSES).

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation,

1 including other law enforcement officers; review of documents and records related to this
2 investigation; communications with others who have personal knowledge of the events and
3 circumstances described herein; and information gained through my training and experience and
4 my discussions with other law enforcement agents who have experience in investigating cases
5 involving child sexual exploitation.

6 5. Because this affidavit is submitted for the limited purpose of establishing
7 probable cause in support of the application for a search warrant, it does not set forth each and
8 every fact that I or others have learned during the course of this investigation. I have set forth
9 only the facts that I believe are relevant to the determination of probable cause to believe that
10 evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES will be found
11 within the SUBJECT FILES.

12 **BACKGROUND ON NCMEC AND CYBERTIPS**

13 6. I know based on my training and experience, that Electronic Service Providers
14 (“ESP”) and/or Internet Service Providers (“ISP,” collectively ISP) typically monitor their
15 services utilized by subscribers. To prevent their communication networks from serving as
16 conduits for illicit activity and pursuant to the terms of user agreements, ISPs routinely and
17 systematically attempt to identify suspected depictions of minors engaged in sexually explicit
18 conduct that may be sent through its facilities. Commonly, customer complaints alert them that
19 an image or video file being transmitted through their facilities likely contains suspected
20 depictions of minors engaged in sexually explicit conduct.

21 7. When an ISP receives such a complaint or other notice of suspected depictions of
22 minors engaged in sexually explicit conduct, they may employ a “graphic review analyst” or an
23 equivalent employee to open and look at the image or video file to form an opinion as to whether
24 what is depicted likely meets the federal criminal definition of depictions of minors engaged in
25 sexually explicit conduct found in 18 USC § 2256, which is defined as any visual depiction,
26 including any photograph, film, video, picture, or computer or computer-generated image or
27 picture, whether made or produced by electronic, mechanical, or other means, of sexually
28 explicit conduct, where: (A) the production of such visual depiction involves the use of a minor
engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer
image, or computer-generated image that is, or is indistinguishable from, that of a minor
engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or

1 modified to appear that an identifiable minor is engaging in sexually explicit conduct. If the
2 employee concludes that the file contains what appears to be depictions of minors engaged in
3 sexually explicit conduct, a hash value of the file can be generated by operation of a
4 mathematical algorithm. A hash value is an alphanumeric sequence that is unique to a specific
5 digital file. Any identical copy of the file will have exactly the same hash value as the original,
6 but any alteration of the file, including even a change of one or two pixels, results in a different
7 hash value. Consequently, an unknown image can be determined to be identical to an original
8 file if it has the same hash value as the original. The hash value is, in essence, the unique
9 fingerprint of that file, and when a match of the “fingerprint” occurs, the file also matches.
10 Several different algorithms are commonly used to hash-identify files, including Message Digest
11 5 (MD5) and Secure Hash Algorithm 1 (SHA-1).

12 8. Hash values are a very reliable method of authenticating files. It can be concluded
13 with an extremely high degree of certainty that two files sharing the same hash value also share
14 identical content. Based on my training and experience, as well as others in this field, I know it is
15 more likely that two humans would share the same biological DNA than for two files to share the
16 same hash value. If even one bit (the smallest measure of data in a file) of a file is changed, the
17 entire hash value of that file changes completely. As an example that demonstrates the
18 uniqueness of a SHA-1 hash, the likelihood of two files having the same SHA-1 hash value is
19 2^{128} or: 1 in 340,000,000,000,000,000,000,000,000,000,000 chance. In an August 6th,
20 2020 article in Live Science, according to Professor Simona Francese, PhD, a forensic scientist
21 and fingerprint expert from Sheffield Hallam University in the United Kingdom, the likelihood
22 of two humans having the same fingerprint is estimated to be: 1 in 64,000,000,000.

23 9. For two different files to have the same hash value is called a *collision*. I know
24 from experience that there have been no documented incidents of a collision involving SHA-1
25 hash values “in the wild” since its creation in 1995. I am, however, aware of a reported collision
26 involving two files sharing the same SHA-1 value in a lab setting. This was done purposely by
27 engineers at Google in 2017 under controlled conditions for the sole purpose of creating this
28 collision. Even with this knowledge in mind, I am confident that the possibility of a suspected
CSAM file reported in a CyberTip having the same hash value as an unrelated, non-criminal file
is extremely unlikely. I believe hash value comparison is a highly reliable method of determining

1 if two files are the same or different, and that a confirmed hash match between two files is a
2 forensic finding on a par with a DNA match or a fingerprint match.

3 10. ISPs typically maintain a database of hash values of files that they have
4 determined to meet the federal definition of depictions of minors engaged in sexually explicit
5 conduct found in 18 USC § 2256. The ISPs typically do not maintain the actual suspect files
6 themselves; once a file is determined to contain suspected depictions of minors engaged in
7 sexually explicit conduct, the file is deleted from their system.

8 11. The ISPs can then use Image Detection and Filtering Process (“IDFP”), Photo
9 DNA (pDNA), or a similar technology which compares the hash values of files embedded in or
10 attached to transmitted files against their database containing what is essentially a catalog of hash
11 values of files that have previously been identified as containing suspected depictions of minors
engaged in sexually explicit conduct.

12 12. When the ISP detects a file passing through its network that has the same hash
13 value as an image or video file of suspected depictions of minors engaged in sexually explicit
14 conduct contained in the database through a variety of methods, the ISP reports that fact to
15 National Center for Missing and Exploited Children (NCMEC) via the latter’s CyberTipline. By
16 statute, an ESP or ISP has a duty to report to NCMEC any apparent depictions of minors
17 engaged in sexually explicit conduct it discovers “as soon as reasonably possible.” 18 U.S.C. §
18 2258A(a)(1). The CyberTip line report transmits the intercepted file to NCMEC. Often that
19 occurs without an ISP employee opening or viewing the file because the files hash value, or
20 “fingerprint,” has already been associated to a file of suspected depictions of minors engaged in
21 sexually explicit conduct. The ISP’s decision to report a file to NCMEC is made solely on the
22 basis of the match of the unique hash value of the suspected depictions of minors engaged in
sexually explicit conduct to the identical hash value in the suspect transmission.

23 13. Most Internet Service Providers keep subscriber records relating to the IP address
24 they assign, and that information is available to investigators. Typically, an investigator has to
25 submit legal process (e.g. subpoena or search warrant) requesting the subscriber information
26 relating to a particular IP address at a specific date and time.

27 14. A variety of publicly available websites provide a public query/response protocol
28 that is widely used for querying databases in order to determine the registrant or assignee of

1 internet resources, such as a domain name or an IP address block. These include WHOIS,
2 MaxMind, arin.net, and other common search tools.

3 15. The act of “downloading” is commonly described in computer networks as a
4 means to receive data to a local system from a remote system, or to initiate such a data transfer.
5 Examples of a remote system from which a download might be performed include a webserver,
6 FTP server, email server, or other similar systems. A download can mean either any file that is
7 offered for downloading or that has been downloaded, or the process of receiving such a file.
8 The inverse operation, “uploading,” refers to the sending of data from a local system to a remote
9 system such as a server or another client with the intent that the remote system should store a
10 copy of the data being transferred, or the initiation of such a process.

11 16. The National Center for Missing and Exploited Children (NCMEC) is a private,
12 non-profit organization established in 1984 by the United States Congress. Primarily funded by
13 the Justice Department, the NCMEC acts as an information clearinghouse and resource for
14 parents, children, law enforcement agencies, schools, and communities to assist in locating
15 missing children and to raise public awareness about ways to prevent child abduction, child
16 sexual abuse and depictions of minors engaged in sexually explicit conduct.

17 17. The Center provides information to help locate children reported missing (by
18 parental abduction, child abduction, or running away from home) and to assist physically and
19 sexually abused children. In this resource capacity, the NCMEC distributes photographs of
20 missing children and accepts tips and information from the public. It also coordinates these
21 activities with numerous state and federal law enforcement agencies. The CyberTipline offers a
22 means of reporting incidents of child sexual exploitation including the possession, manufacture,
23 and/or distribution of depictions of minors engaged in sexually explicit conduct; online
24 enticement; child prostitution; child sex tourism; extra familial child sexual molestation;
25 unsolicited obscene material sent to a child; and misleading domain names, words, or digital
26 images.

27 18. Any incidents reported to the CyberTipline online or by telephone go through this
28 three-step process: CyberTipline operators review and prioritize each lead; NCMEC’s Exploited
Children Division analyzes tips and conducts additional research; The information is accessible
to the FBI, ICE, and the USFIS via a secure Web connection. Information is also forwarded to

1 the ICACs and pertinent international, state, and local authorities and, when appropriate, to the
2 ESP.

3
4 **SUMMARY OF PROBABLE CAUSE**

5 19. This case involves the investigation of Nathan Hall, a resident of the Western
6 District of Washington. Between 2015 and 2024, the FBI received multiple complaints about
7 Hall's online activity. In August 2024, FBI obtained warrants to search Hall's home and person
8 for evidence of, among other things, communicating interstate threats and possession of child
9 sexual abuse material. FBI seized multiple digital devices, and the review of these devices is
ongoing.

10 20. On July 29, 2024, I received a Cybertip report from NCMEC that was submitted
11 by ESP X reporting that one of its users had uploaded suspected child pornography to its servers.
12 According to X, a review of the account prompted by a June 2024 administrative subpoena
13 seeking subscriber information for this X account resulted in the discovery of apparent child
14 pornography. X submitted a Cybertip report to NCMEC that included the SUBJECT FILES. X
15 also provided the following subscriber information associated with this account:

16 Username AlexAnderHare17
17 Email Nathanhall100@hotmail.com
18 Phone 360-600-4184

19 21. X also indicated that it did not view the SUBJECT FILES, so I am seeking
20 authority to open and examine them.


21 22. I know from my training and experience that when X submits a Cybertip, it
22 provides a copy of account content associated with the user that is the subject of the tip. In
23 addition to the files of suspected child pornography, this may include content such as direct
24 messages, postings, and other information that my help identify the user of the account.
25
26
27
28

1 **CONCLUSION**

2 23. Based on the foregoing, I believe there is probable cause to conclude that
3 evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES, are located
4 within the SUBJECT FILES as more fully described in Attachment A to this Affidavit. I
5 therefore request that the Court issue a warrant authorizing a search of the SUBJECT FILES for
6 the items more fully described in Attachment B and the seizure of any such items found therein.

7
8 
9 NATALIE LEAVITT
10 Special Agent, FBI
11

12 The above-named agent provided a sworn statement attesting to the truth of the contents
13 of the foregoing affidavit on the 30th day of January, 2025.
14

15
16 
17 S. KATE VAUGHAN
18 United States Magistrate Judge
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A

Description of Property to be Searched

The following SUBJECT FILES

AlexAnderHare17-327816241-2024-07-29-18-15-25-79217672.zip

2Q9n0uXI.jpg

provided by X Corp to the National Center for Missing and Exploited Children with
CyberTipline Report #197075910, which are stored on an encrypted thumb drive currently
located at the FBI office in Bellingham, Washington.

ATTACHMENT B
ITEMS TO BE SEIZED

All information that constitutes evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of/Access with Intent to View Child Pornography) which may be found in the SUBJECT FILES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct;
2. Information about the SUBJECT FILES related to the timing or circumstances of their creation and transmission; in any format or media;
3. Information concerning the identity of any individuals depicted in the SUBJECT FILES
4. Information or data that, including direct messages, postings, photos, or other account content that identifies the user(s) of the X account associated with the SUBJECT FILES.